Disjoint difference families and their applications

By

S.-L. Ng and M.B. Paterson

Birkbeck Pure Mathematics Preprint Series | Preprint Number 14

www.bbk.ac.uk/ems/research/pure/preprints

Disjoint difference families and their applications

S. -L. Ng, M. B. Paterson

September 16, 2015

Abstract

Difference sets and their generalisations to difference families arise from the study of designs and many other applications. Here we give a brief survey of some of these applications, noting in particular the diverse definitions of difference families and the variations in priorities in constructions. We propose a definition of disjoint difference families that encompasses these variations and allows a comparison of the similarities and disparities. We then focus on two constructions of disjoint difference families arising from frequency hopping sequences and showed that they are in fact the same. We conclude with a discussion of the notion of equivalence for frequency hopping sequences and for disjoint difference families.

1 Introduction

Difference sets and their generalisations to difference families arise from the study of designs and many other applications. In particular, the generalisation of difference sets to internal and external difference families arises from many applications in communications and information security. Roughly speaking, a difference family consists of a collection of subsets of an abelian group, and internal differences are the differences between elements of the same subsets, while external differences are the differences between elements of distinct subsets. Most of the definitions do not coincide exactly with each other, understandably since they arise from diverse applications, and the priorities of maximising or minimising various parameters are also understandably divergent. However, there is enough overlap in these definitions to warrant a study of how they relate to each other, and how the construction of one family may inform the construction of another. One of the aims of this paper is to perform a brief survey of these difference families, noting the variations in definitions and priorities, and to propose a definition that encompasses these definitions and allows a more unified study of these objects.

One particular class of internal difference family arises from frequency hopping (FH) sequences. FH sequences allow many transmitters to send messages simultaneously using a limited number of channels and it transpires that the property of how efficiently one can send messages has to do with the number of internal differences in a collection of subsets of frequency channels. The seminal paper of Lempel and Greenberger [8] gave optimal FH sequences using transformations of linear feedback shift register (LFSR) sequences. In another paper by Fujihara *et al.* [5] various families of FH sequences were constructed using designs with particular automorphisms, and the question was raised there as to whether these constructions are the same as the LFSR constructions in [8]. Here we show a correspondence between one particular family of constructions in [5] and that of [8].

The relationship between the equivalence of difference families and the equivalence of the designs and codes that arise from them has been much studied. Here we will focus on the notion of equivalence for frequency hopping sequences and for disjoint difference families, and we will point to further open questions in this area.

1.1 Definitions

Let $\mathcal{G}$ be an abelian group[1] of size v, and let $Q_0, \ldots, Q_{q-1}$ be disjoint subsets of $\mathcal{G}$, $|Q_i| = k_i$, $i = 0, \ldots, q-1$. We will call $(\mathcal{G}; Q_0, \ldots, Q_{q-1})$ a *disjoint difference family* $\mathrm{DDF}(v; k_0, \ldots, k_{q-1})$ over $\mathcal{G}$ with the following *external* $\mathcal{E}(\cdot)$ and *internal* $\mathcal{I}(\cdot)$ *differences*:

[1]The Handbook of Combinatorial Designs [2] has more material on difference families defined on non-abelian groups, but we will focus on abelian groups here since most of the applications we examine here use abelian groups.

$$
\begin{aligned}
\mathcal{E}_{i,j}(d) &= \{(a,b) \,:\, a-b=d, a\in Q_i, b\in Q_j\},\\
\mathcal{E}_i(d) &= \{(a,b) \,:\, a-b=d, a\in Q_i, b\in Q_j, j=0,\ldots,q-1, j\neq i\},\\
\mathcal{E}(d) &= \{(a,b) \,:\, a-b=d, a\in Q_i, b\in Q_j, i,j=0,\ldots,q-1, i\neq j\},\\
\mathcal{I}_i(d) &= \{(a,b) \,:\, a-b=d, a,b\in Q_i, a\neq b\},\\
\mathcal{I}(d) &= \{(a,b) \,:\, a-b=d, a,b\in Q_i, a\neq b, i=0,\ldots,q-1\}.
\end{aligned}
$$

We will call the DDF *uniform* if all the Q_i are of the same size, and we will say it is a *perfect*[2] internal (or external) DDF if $|\mathcal{I}(d)|$ (or $|\mathcal{E}(d)|$) is a constant for all $d\in\mathbb{Z}_v^*$. We will call the DDF a *partition type* DDF if $\{Q_0,\ldots,Q_{q-1}\}$ is a partition of $\mathcal{G}$.

Remark 1.1. As mentioned before and as will be pointed out in Section 2, there is by no means a consensus on the terms used to describe a DDF. Here we point out the disparity between our terms and those of [2], and in Section 2 we will point out the differences as they arise. In particular, the definition of difference family in [2] stipulates that the subsets Q_i are all of the same size, but does not insist that they are disjoint. We have defined a DDF to consist of disjoint subsets (of varying sizes) because we want to be able to define *external* differences. Using the term *uniform* to describe the subsets Q_i being of the same size is consistent with terminology used in design theory. □

Example 1.2. A (v,k,λ)-difference set Q_0 over $\mathbb{Z}_v$ is a perfect internal DDF$(v;k)$ with $|\mathcal{I}(d)|=\lambda=k(k-1)/(v-1)$. If we let $Q_1=\mathbb{Z}_v\setminus Q_0$ then $(\mathbb{Z}_v;Q_0,Q_1)$ is an internal DDF$(v;k,v-k)$ with $|\mathcal{I}_0(d)|=\lambda$ and $|\mathcal{I}_1(d)|=v-2k+\lambda$ for all $d\in\mathbb{Z}_v^*$. In fact, $(\mathbb{Z}_v;Q_0,Q_1)$ has $|\mathcal{I}(d)|=v-2k+2\lambda$ and $|\mathcal{E}(d)|=v(v-1)-(v-2k+2\lambda)$ and is a perfect internal and external DDF.

For example, the $(7,3,1)$ difference set $Q_0=\{0,1,3\}\subseteq\mathbb{Z}_7$. We have $|\mathcal{I}(d)|=1$. Let $Q_1=\mathbb{Z}_7\setminus Q_0=\{2,4,5,6\}$. Then we have $|\mathcal{I}_1(d)|=2$, $|\mathcal{E}_0(d)|=|\mathcal{E}_1(d)|=2$ and $|\mathcal{E}(d)|=4$ for all $d\in\mathbb{Z}_7^*$. □

It is not hard to see that a perfect partition type internal DDF is also a perfect partition type external DDF and vice versa. However, this is not generally true for DDFs that are not partition type:

Example 1.3. Let $\mathcal{G}=\mathbb{Z}_{25}$, $Q_0=\{1,2,3,4,6,15\}$, $Q_1=\{5,9,10,14,17,24\}$. This is a perfect external DDF$(25;6,6)$ with $|\mathcal{E}(d)|=3$ for all $d\in\mathbb{Z}_{25}^*$ given in [6]. However, it is not a perfect internal DDF:

$$
|\mathcal{I}(d)| = \begin{cases} 4 & \text{for} \quad d=1,24,\\ 2 & \text{for} \quad d=7,9,10,15,16,18,\\ 1 & \text{for} \quad d=6,8,17,19,\\ 3 & \text{for} \quad \text{all other } d. \end{cases}
$$

□

In many codes and sequences [5, 3, 6, 11, 1], desirable properties can be expressed in terms of (some) external or internal differences of DDFs. We give a brief survey of these applications and the properties required of the DDFs in the next section.

2 Disjoint difference families in applications

This is not intended to be a comprehensive survey of where disjoint difference families arise in applications, nor of each application. We want to show that these objects arise in many areas of communications and information security research and that a study of their various properties may be useful in making advances in these fields.

2.1 Frequency hopping (FH) sequences [5]

Let $F=\{f_0,\ldots,f_{q-1}\}$ be a set of frequencies used in a frequency hopping multiple access communication system [4]. A frequency hopping (FH) sequence X of length v over F is simply $X=(x_0,x_1,\ldots,x_{v-1})$, $x_i\in F$, specifying that frequency x_i should be used at time i. If two FH sequences use the same frequency at the same time (a collision), the messages sent at that time may be corrupted. Collisions are given by Hamming correlations: if a single sequence together with all its cyclic shifts are used then the number of collisions is given by its auto-correlation values (the number of positions in which cyclic shifts agree with the original sequence). Such a sequence X may also be viewed in a combinatorial way: Define Q_i, $i=0,\ldots,q-1$, as subsets of $\mathbb{Z}_v$, with $j\in Q_i$ if $x_j=i$. Hence each Q_i correspond to a frequency f_i, and the elements of Q_i are the positions in

[2]The term *perfect* is used in [2] to refer to a specific type of difference family where half the differences cover half the ground set. Our usage is found in [13] in relation to self-synchronising codes.

X where f_i is used. (For example, the frequency hopping sequence $X = (0, 0, 1, 0, 1, 1, 1)$ over $F = \{0, 1\}$ gives the DDF of Example 1.2.) In [5] it is shown that an FH sequence $(x_0, x_1, \ldots, x_{v-1})$ with out-of-phase autocorrelation value of at most λ exists if and only if $(\mathbb{Z}_v; Q_0, \ldots, Q_{q-1})$ is a partition type $\mathrm{DDF}(v; k_0, \ldots, k_{q-1})$ with $\mathcal{I}(d)$ satisfying

$$|\mathcal{I}(d)| \leq \lambda \text{ for all } d \in \mathbb{Z}_v^*.$$

In [5] $(\mathbb{Z}_v; Q_0, \ldots, Q_{q-1})$ is called a partition type difference packing.

The aim in FH sequences design is to minimise collisions: we would like λ to be small. Lempel and Greenberger [8] proved a lower bound for λ and constructed optimal sequences meeting this bound using transformations of m-sequences (more details in Section 4.1). In [5] Fuji-Hara *et al.* also provided many examples of optimal sequences using designs with certain types of automorphisms. Later in this paper we will show that one of the Fuji-Hara *et al.* constructions gives the same sequences as those constructed by Lempel and Greenberger.

2.2 Weak algebraic manipulation detection (AMD) codes [3]

Consider a device that is capable of storing an element x from an abelian group $\mathcal{G}$ of order v. An adversary cannot obtain information about x, but can choose an element $d \in \mathcal{G}$ and add it the stored data, thus changing the value. This is called an algebraic manipulation. Suppose S is the set of k sources, and $\mathcal{G}$ is an abelian group of order v. Let E be a probabilistic encoding map $E\colon S \to \mathcal{G}$, and let D be a deterministic decoding map $D\colon \mathcal{G} \to S \cup \{\perp\}$ such that $D(E(s)) = s$ for all $s \in S$. The pair (E, D) is a weak (k, v, ϵ)-AMD (algebraic manipulation detection) code if for every $d \in \mathcal{G}$, and for any s sampled uniformly at random from S, the probability that $D(E(s) + d) \notin \{s, \perp\}$ is at most ϵ. Thus, a weak AMD code maps a source to a value in $\mathcal{G}$ in such a way that an algebraic manipulation goes undetected with a bounded probability. AMD codes are studied also in the context of secret sharing schemes and robust fuzzy extractors. We refer the reader to [3] for references. In [3], it is shown that a weak (k, v, ϵ)-AMD code is equivalent to a $\mathrm{DDF}(v; k)$ with

$$|\mathcal{I}(d)| \leq \lambda,\ \lambda \leq \epsilon k \ \text{ for all } d \in \mathbb{Z}_v^*.$$

In [3] these are called (v, k, λ)-bounded difference sets. It is easy to see that these are generalisations of difference sets, allowing general abelian groups and allowing inequality for the number of differences.

Bounds on the adversary's success probability in a weak AMD code are given in [3] and several families with good asymptotic properties are constructed using vector spaces. Additional bounds are given in [12], and constructions and characterisations are given relating weak AMD codes that are optimal with respect to these bounds to a variety of types of external DDF. It is desirable to minimise the tag length ($\log v - \log k$, the number of redundant bits) as well as ϵ.

2.3 Self-synchronising codes [6]

Self-synchronising codes are also called comma-free codes and have the property that no codeword appears as a substring of two concatenated codewords. This allows for synchronisation without external help. Codes achieving self-synchronisation in the presence of up to $\lfloor \frac{\lambda-1}{2} \rfloor$ errors can be constructed from a $\mathrm{DDF}(v; k_0, \ldots, k_{q-1})$ $(\mathbb{Z}_v; Q_0, \ldots, Q_{q-1})$ with $|\mathcal{E}(d)| \geq \lambda$. In [6], this DDF is called a difference system of sets of index λ over $\mathbb{Z}_v$. We refer the reader to [6] for references to the origin and motivation of this definition and for bounds and constructions. There are constructions from the partitioning of cyclic difference sets and partitioning of hyperplanes in projective geometry, as well as iterative constuctions using external and internal DDF. The sets $Q_0, \ldots, Q_{q-1}$ give the markers for self-synchronisation and are a redundancy, hence we would like $k = \sum_{i=0}^{q-1} k_i$ to be small. Other optimisation problems include reducing the rate k/v, reducing λ, and reducing the number q of subsets.

2.4 Splitting A-codes and robust secret sharing schemes [11]

In authentication codes (A-codes), a transmitter and a receiver shares an encoding rule e, chosen according to some specified probability distribution. To authenticate a source state s, the transmitter encodes s using e and sends the resulting message $m = e(s)$ to the receiver. The receiver recieves a message m' and accepts it if $m' = e(s)$. In a splitting A-code, the message is computed with an input of randomness so that a source state is not uniquely mapped to a message. We refer to [11] for further background. It is shown in [11] that optimal splitting A-codes can be constructed from a perfect uniform external $\mathrm{DDF}(v; k_0 = k, \ldots, k_{q-1} = k)$ with $|\mathcal{E}(d)| = 1$. This gives an A-code with q source states, v encoding rules, v messages, and each source state can be mapped to k valid messages. This DDF is called an external difference family in [11], and they are also used to construct optimal secret sharing schemes secure against cheaters. The probability of an adversary

successfully impersonating the transmitter is given by kq/v and the probability of successfully substituting a message being transmitted is given by $1/kq$ (which also happens to equal $k(q-1)/(v-1)$ in this particular context). These are parameters to be minimised.

2.5 Stong algebraic manipulation detection (AMD) codes [3]

A stronger form of AMD (see Section 2.2) says that for every source $s \in S$ and every element $d \in \mathcal{G}$, the probability that $D(E(s)+d) \notin \{s, \perp\}$ is at most ϵ. Write $Q_i = \{g \in \mathcal{G} \ : \ D(g) = s_i\}$ for each $s_i \in S$, $i = 0, \ldots, k-1$, and $|Q_i| = k_i$. In the case where the encoding $E(s_i)$ is uniformly distributed over Q_i for every s_i, $(\mathcal{G}; Q_0, \ldots, Q_{k-1})$ forms a DDF$(v; k_0, \ldots, k_{k-1})$ with $|\mathcal{E}_i(d)| \leq \lambda_i = \epsilon k_i$ and $|\mathcal{E}(d)| \leq \lambda = \sum_{i=0}^{k-1} \lambda_i$. Constructions from vector spaces and caps in projective space are given in [3]. Additional bounds and characterisations are given in [12].

2.6 Optical orthogonal codes (OOCs) [1]

Optical orthogonal codes (OOCs) are sequences arising from applications in code-division multiple access in fibre optic channels. OOC with low auto- and cross-correlation values allow users to transmit information efficiently in an asynchronous environment. A $(v, w, \lambda_a, \lambda_c)$-OOC of size q is a family of q $(0,1)$-sequences $\{X_0, \ldots, X_{q-1}\}$ of length v, weight w, such that auto-correlation values are at most λ_a and cross-correlation values are at most λ_c. For each sequence X_i, let Q_i be the set of integers modulo v denoting the positions of the non-zero bits. Then $(\mathbb{Z}_v; Q_0, \ldots, Q_{q-1})$ is a uniform DDF$(v; k_0 = w \ldots, k_{q-1} = w)$ with

$$\begin{aligned} |\mathcal{I}_i(d)| &\leq \lambda_a, \\ |\mathcal{E}_{i,j}(d)| &\leq \lambda_c \text{ for all } d \in \mathbb{Z}_v^*. \end{aligned}$$

Background and motivation to the study of OOC are given in [1] including constructions from designs, algebraic codes and projective geometry.

3 A geometrical look at a perfect partition type disjoint difference family

In [5] a perfect partition type DDF$(q^n - 1; k_0 = q-1, k_1 = q, \ldots, k_{q^n-1-1} = q)$ over $\mathbb{Z}_{q^n-1}$ was constructed from line orbits of a cyclic perspectivity τ in the n-diminsional projective space $PG(n,q)$ over GF(q). In [8] another construction with the same parameters was given. In the next section we will show a correspondence between the two constructions. Before that we will describe in greater detail the the construction of [5, Section III].

An n-dimensional projective space $PG(n,q)$ over the finite field of order q admits a cyclic group of perspectivities $\langle\tau\rangle$ of order $q^n - 1$ that fixes a hyperplane $\mathcal{H}_\infty$ and a point $\infty \notin \mathcal{H}_\infty$. (We refer the reader to [7] for properties of projective spaces and their automorphism groups.) This group $\langle\tau\rangle$ acts transitively on the points of $\mathcal{H}_\infty$ and regularly on the points of $PG(n,q) \setminus (\mathcal{H}_\infty \cup \{\infty\})$. We will call the points (and spaces) not contained in $\mathcal{H}_\infty$ the affine points (and spaces).

The point orbits of $\langle\tau\rangle$ are $\{\infty\}$, $\mathcal{H}_\infty$, and $PG(n,q) \setminus (\mathcal{H}_\infty \cup \{\infty\})$. Dually, the hyperplane orbits are $\mathcal{H}_\infty$, the set of all hyperplanes through ∞, and the set of all hyperplanes of $PG(n,q) \setminus \mathcal{H}_\infty$ not containing ∞. Line orbits under $\langle\tau\rangle$ are:

(A) One orbit of affine lines through ∞ - this orbit has length $\frac{q^n-1}{q-1}$; and

(B) $\frac{q^{n-1}-1}{q-1}$ orbits of affine lines not through ∞ - each orbit has length $q^n - 1$, and $\langle\tau\rangle$ acts regularly on each orbit; and

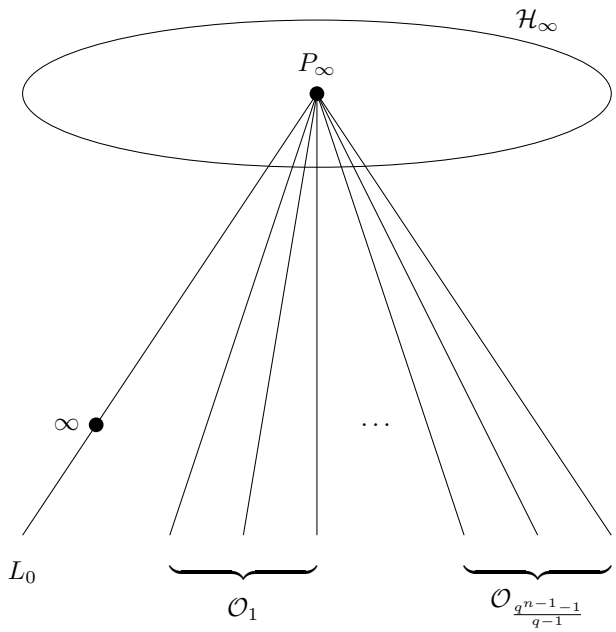
(C) One orbit of lines contained in $\mathcal{H}_\infty$.

A set of parallel (affine) lines through a point $P_\infty \in \mathcal{H}_\infty$ consists of one line L_0 from the orbit of type (A) and $q-1$ lines from each of the $(q^{n-1}-1)/(q-1)$ orbits of type (B). We will write this set of q^{n-1} lines $\mathcal{P} = \{L_0, L_1, \ldots, L_{q^{n-1}-1}\}$ as follows (See Figure 1):

- L_0, a line through ∞ and $P_\infty \in \mathcal{H}_\infty$;
- $\mathcal{O}_i = \{L_{(i-1)(q-1)+1}, L_{(i-1)(q-1)+2}, \ldots, L_{(i-1)(q-1)+(q-1)}\}$, $i = 1, \ldots, \frac{q^{n-1}-1}{q-1}$, each $\mathcal{O}_i$ belonging to a different orbit under $\langle\tau\rangle$.

We consider the two types of $d \in \mathbb{Z}_{q^n-1}^*$ depending on the action of τ^d on L_0:

Figure 1: The parallel class $\mathcal{P}$.



(I) There are $q-2$ τ^d, $d \in \mathbb{Z}^*_{q^n-1}$, fixing the line L_0 (and the points P_∞ and ∞) and permuting the points of L_0. These τ^d permute but do not fix the lines within each $\mathcal{O}_i$. Hence we have, for these $d \in \mathbb{Z}^*_{q^n-1}$,

$$L_0^{\tau^d} \cap L_0 = L_0 \text{ and } L_i^{\tau^d} \cap L_i = \{P_\infty\}. \tag{1}$$

(II) The remaining $(q^n-1)-(q-2)$ τ^d map lines in $\mathcal{P}$ to affine lines not in $\mathcal{P}$. Hence we have

$$L_0^{\tau^d} \cap L_0 = \{\infty\} \text{ and } |L_i^{\tau^d} \cap L_i| = 0 \text{ or } 1. \tag{2}$$

Without loss of generality consider $L_1 \in \mathcal{O}_1$. Suppose $|L_1^{\tau^d} \cap L_1| = 1$, say $L_1^{\tau^d} \cap L_1 = \{P\}$. Let $L_k \in \mathcal{O}_1$ be another line in the same orbit as L_1, so there is a d_k such that $L_1^{\tau^{d_k}} = L_k$. It is not hard to see that $\{P^{\tau^{d_k}}\} = L_k^{\tau^d} \cap L_k$, since

$$P \in L_1 \Rightarrow P^{\tau^{d_k}} \in L_1^{\tau^{d_k}} = L_k,$$
$$P \in L_1^{\tau^d} \Rightarrow P^{\tau^{d_k}} \in (L_1^{\tau^d})^{\tau^{d_k}} = (L_1^{\tau^{d_k}})^{\tau^d} = L_k^{\tau^d}.$$

Hence for any orbit $\mathcal{O}_i$, if $|L_j^{\tau^d} \cap L_j| = 1$ for some $L_j \in \mathcal{O}_i$ then $|L_k^{\tau^d} \cap L_k| = 1$ for all $L_k \in \mathcal{O}_i$

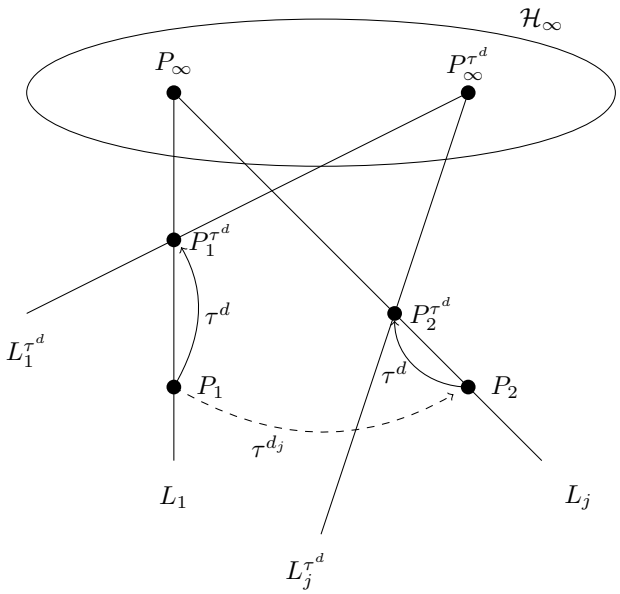
Now, suppose again that $|L_1^{\tau^d} \cap L_1| = 1$. Let P_1 be the point on L_1 such that $P_1^{\tau^d} \in L_1^{\tau^d} \cap L_1$. Consider $L_j \in \mathcal{O}_k$, $k \neq 1$. Suppose $|L_j^{\tau^d} \cap L_j| = 1$. Let P_2 be the point on L_j such that $P_2^{\tau^d} \in L_j^{\tau^d} \cap L_j$. (See Figure 2.) Since $\langle\tau\rangle$ is transitive on affine points (excluding ∞), there is a d_j such that $P_1^{\tau^{d_j}} = P_2$. Then

$$(P_1^{\tau^d})^{\tau^{d_j}} = (P_1^{\tau^{d_j}})^{\tau^d} = P_2^{\tau^d}.$$

This means that τ^{d_j} maps P_1 to P_2 and $P_1^{\tau^d}$ to $P_2^{\tau^d}$ and hence maps the line L_1 to L_j. But this is a contradiction since L_1 and L_j belong to different orbits under $\langle\tau\rangle$. Hence if $|L_j^{\tau^d} \cap L_j| = 1$ for any L_j in some orbit $\mathcal{O}_i$ then $|L_k^{\tau^d} \cap L_k| = 0$ for all L_k in all other orbits.

It is also clear that for any L_i in any orbit, there is a d such that $|L_i^{\tau^d} \cap L_i| = 1$, because $\langle\tau\rangle$ is transitive on affine points (excluding ∞). Indeed, $\langle\tau\rangle$ acts regularly on these points, so that for any pair of points (P, Q) on L_i there is a unique d such that $P^{\tau^d} = Q$. There are $q(q-1)$ pairs of points and so there are $q(q-1)$ such values of d. These $q(q-1)$ values of d for each $\mathcal{O}_i$ in $\mathcal{P}$, together with the $q-2$ values of d where τ^d that fixes L_0, account for all of $\mathbb{Z}^*_{q^n-1}$.

Figure 2: L_1, L_j in different orbits



Now, the points of $PG(n,q) \setminus (\mathcal{H}_\infty \cup \{\infty\})$ can be represented as $\mathbb{Z}_{q^n-1}$ as follows: pick an arbitrary point P_0 to be designated 0. The point $P_0^{\tau^i}$ corresponds to $i \in \mathbb{Z}_{q^n-1}$. The action of τ^d on any point P is thus represented as $P + d$. Affine lines are therefore q-subsets of $\mathbb{Z}_{q^n-1}$. Let $Q_0 \subseteq \mathbb{Z}_{q^n-1}$ contain the points of $L_0 \setminus \{\infty\}$, and let Q_i contain the points of L_i. It follows from the intersection properties of the lines (properties (1), (2)) that $\{Q_0, \ldots, Q_{q^{n-1}-1}\}$ forms a perfect partition type DDF$(q^n - 1; q-1, q, \ldots, q)$ over $\mathbb{Z}_{q^n-1}$, with $|\mathcal{I}(d)| = q - 1$ for all $d \in \mathbb{Z}_{q^n-1}^*$.

3.1 A perfect external DDF

Given that a partition type perfect internal DDF over $\mathbb{Z}_v$ with $|\mathcal{I}(d)| = \lambda$ must be a perfect external DDF with $|\mathcal{E}(d)| = v - \lambda$, the intersection properties $|L_i^{\tau^d} \cap L_j|$, $i \neq j$ can be deduced as follows for the two different types (I), (II) of d:

(I) For the $q-2$ τ^d of type (I) fixing L_0, we have:

- (a) L_0 is fixed, so $|L_0^{\tau^d} \cap L_i| = 0$ for all $L_i \neq L_0$.
- (b) If L_i and L_j are in different orbits then $|L_i^{\tau^d} \cap L_j| = 0$ (since τ^d fixes $\mathcal{O}_i$).
- (c) If L_i and L_j are in the same orbit, then since τ^d acts regularly on an orbit of type (B), there is a unique d that maps L_i to L_j, so $|L_i^{\tau^d} \cap L_j| = q$, and for all other L_k in the same orbit, $|L_i^{\tau^d} \cap L_k| = 0$. This applies to each orbit, so that for each of the $q-2$ values of d, there are $((q^{n-1}-1)/(q-1)) \times (q-1) = q^{n-1} - 1$ cases where $|L_i^{\tau^d} \cap L_j| = q$.

(II) For the $(q^n - 1) - (q-2)$ τ^d of type (II) not fixing L_0, we have:

- (a) Pick any point $P \in L_0 \setminus \{\infty\}$, $P^{\tau^d} \in L_i$ for some $L_i \neq L_0$, so $|L_0^{\tau^d} \cap L_i| = 1$ for some L_i. There are $q-1$ points on $L_0 \setminus \{\infty\}$, so there are $q-1$ lines L_i such that $|L_0^{\tau^d} \cap L_i| = 1$.
- (b) Consider $L_i \neq L_0$. Take any point $P \in L_i$. We have $P^{\tau^d} \in L_j$ for some L_j, so $|L_i^{\tau^d} \cap L_j| = 1$. This applies for all L_i, so that for any of the $(q^n - 1) - (q-2)$ values of d, there are $(q^{n-1} - 1)q$ cases of $|L_i^{\tau^d} \cap L_j| = 1$, $q-1$ of which are when $L_j = L_i$.

Defining the sets $Q_0, \ldots, Q_{q^{-1}}$ as before, we see that $\{Q_0, \ldots, Q_{q^{-1}}\}$ forms a perfect partition type DDF with $\mathcal{E}(d) = q(q^{n-1} - 1)$.

4 A correspondence between two difference families

In [5], Fuji-Hara *et al.* constructed the perfect partition type DDF($q^n - 1; q - 1, q, \ldots, q$) over $\mathbb{Z}_{q^n-1}$ with $|\mathcal{I}(d)| = q - 1$ described in Section 3. Using parallel t-dimensional subspaces (we described the case when $t = 1$), perfect partition type DDF($q^n - 1; q^t - 1, q^t, \ldots, q^t$) with $|\mathcal{I}(d)| = q^t - 1$ can also be constructed.

This construction gives DDF of the same parameters as those constructed using m-sequences in [8], though [8] restricted their constructions to the case when q is a prime. It was asked in [5] whether these are "essentially the same" constructions. In this section we show a correspondence between these two constructions, and in Section 5 we discuss what "essentially the same" might mean. This correspondence also shows that the restriction to q prime in [8] is unnecessary.

4.1 The Lempel-Greenberger m-sequence construction

We refer the reader to [9] for more details on linear recurring sequence. Here we sketch an introduction. Let $(s_t) = s_0 s_1 s_2 \ldots$ be a sequence of elements in GF(q), q a prime power, satisfying the n-th order linear recurrence relation

$$s_{t+n} = c_{n-1}s_{t+n-1} + c_{n-2}s_{t+n-2} + \cdots + c_0 s_t,\ c_i \in \mathrm{GF}(q),\ c_{n-1} \neq 0.$$

Then (s_t) is called an (nth order) linearly recurring sequence in GF(q). Such a sequence can be generated using a *linear feedback shift register (LFSR)*. An LFSR is a device with with n *stages*, which we denote by $S_0, \ldots, S_{n-1}$. Each stage is capable of storing one element of GF(q). The contents s_{t+i} of all the registers S_i ($0 \leq i \leq n-1$) at a particular time t is known as the *state* of the LFSR at time t. We will write it either as $s(t, n) = s_t s_{t+1} \ldots s_{t+n-1}$ or as a vector $\mathbf{s}_t = (s_t, s_{t+1}, \ldots, s_{t+n-1})$. The state $\mathbf{s}_0 = (s_0, s_1, \ldots, s_{n-1})$ is the *initial state*.

At each clock cycle, an output from the LFSR is extracted and the LFSR is updated as described below.

- The content s_t of the stage S_0 is output and forms part of the *output sequence*.
- For all other stages, the content s_{t+i} of stage S_i is moved to stage S_{i-1} ($1 \leq i \leq n-1$).
- The new content s_{t+n} of stage S_{n-1} is the value of the **feedback function**

$$f(s_t, s_{t+1}, \ldots, s_{t+n-1}) = c_0 s_t + c_1 s_{t+1} + \cdots c_{n-1} s_{t+n-1},\ c_i \in \mathrm{GF}(q).$$

  The new state is thus $\mathbf{s}_{t+1} = (s_{t+1}, s_{t+2}, \ldots, s_{t+n})$. The constants $c_0, c_1, \ldots, c_{n-1}$ are known as the *feedback coefficients* or *taps*.

A diagrammatic representation of an LFSR is given in Figure 3.

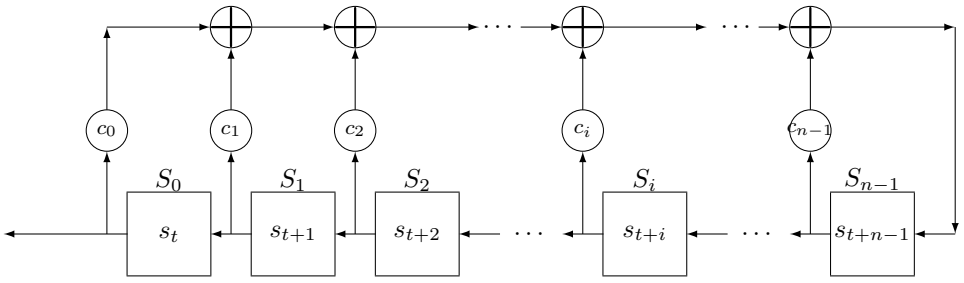


Figure 3: Linear Feedback Shift Register

The *characteristic polynomial* associated with the LFSR (and the linear recurrence relation) is

$$f(x) = x^n - c_{n-1}x^{n-1} - c^{n-2}x^{n-2} - \cdots - c_0.$$

The state at time $t + 1$ is also given by $\mathbf{s}_{t+1} = \mathbf{s}_t C$, where C is the *state update matrix* given by

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & \dots & 0 & c_1 \\ 0 & 1 & \dots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & c_{n-1} \end{pmatrix}.$$

A sequence (s_t) generated by an n-stage LFSR is periodic and has maximum period $q^n - 1$. A sequence that has maximum period is referred to as an *m-sequence*. An LFSR generates an m-sequence if and only if its characteristic polynomial is primitive. An m-sequence contains all possible non-zero states of length n, hence we may use, without loss of generality, the impulse response sequence (the sequence generated using initial state $(0 \cdots 01)$).

Let $S = (s_t) = s_0 s_1 s_2 \dots$ be an m-sequence over a prime field GF(p) generated by an n-stage LFSR with a primitive characteristic polynomial $f(x)$. Let $s(t,k) = s_t s_{t+1} \dots s_{t+k-1}$ be a subsequence of length k starting from s_t.

The σ_k-transformations, $1 \le k \le n-1$ introduced in [8] are described as follows:

$$\sigma_k : s(t,k) = s_t s_{t+1} \dots s_{t+k-1} \to \sum_{i=0}^{k-1} s_{t+i} p^i \in \mathbb{Z}_{p^k} = \{0, 1, \dots, p^k - 1\}.$$

We write the σ_k-transform of S as $U = (u_t)$, $u_t = s(t,k)\sigma_k$, which is a sequence over $\mathbb{Z}_{p^k}$.

In [8, Theorem 1] it is shown that the sequence U forms a frequency hopping sequence with out-of-phase auto-correlation value of $p^{n-k} - 1$, and hence a partition type perfect DDF with $|\mathcal{I}(d)| = p^{n-k} - 1$ (Section 2.1). We see in the next section that this corresponds to the geometric construction of [5] described in Section 3.

4.2 A geometric view of the Lempel-Greenberger m-sequence construction.

We refer the reader to [7] for details about coordinates in finite projective spaces over GF(q). Here we only sketch what is necessary to describe the m-sequence construction of Section 4.1 from the projective geometry point of view.

Let $PG(n,q)$ be an n-dimensional projective space over GF(q). Then we may write

$$PG(n,q) = \{(x_0, x_1, \dots, x_n) \mid x_i \in \text{GF}(q) \text{ not all zero}\},$$

with the proviso that $\rho(x_0, x_1, \dots, x_n)$, $\rho \in \text{GF}(q) \setminus \{0\}$ all refer to the same point. Dually a hyperplane of $PG(n,q)$ is written as $[a_0, a_1, \dots, a_n]$, $a_i \in \text{GF}(q)$ not all zero, and contains the points $(x_0, x_1, \dots, x_n)$ satisfying the equation

$$a_0 x_0 + a_1 x_1 + \cdots + a_n x_n = 0.$$

Clearly $\rho[a_0, a_1, \dots, a_n]$, $\rho \in \text{GF}(q) \setminus \{0\}$ refers to the same hyperplane. A k-dimensional subspace is specified by either the points contained in it, or the equations of the $n-k$ hyperplanes containing it.

Now, let $S = (s_t) = s_0 s_1 s_2 \dots$ be an m-sequence over GF(p), p prime, generated by an n-stage LFSR with a primitive characteristic polynomial $f(x)$ and state update matrix C, as described in the previous section. For $t = 0, \dots, p^n - 2$, let $P_t = (s_t, s_{t+1}, \dots, s_{t+n-1}, 1)$. Then the set $\mathcal{O} = \{P_t \mid t = 0, \dots p^n - 2\}$ are the points of $PG(n,p) \setminus (\mathcal{H}_\infty \cup \{\infty\})$ where $\mathcal{H}_\infty$ is the hyperplane $x_n = 0$ and ∞ is the point $(0, \dots, 0, 1)$.

Let τ be the projectivity defined by

$$A = \begin{pmatrix} & & & 0 \\ & C & & \vdots \\ & & & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Then τ fixes $\mathcal{H}_\infty$ and ∞, acts regularly on $\mathcal{O} = \{P_t \mid t = 0, \dots p^n - 2\}$, and maps P_t to P_{t+1}. Now we consider what a σ_k-transformation means in $PG(n,p)$.

Firstly we consider σ_{n-1}. This takes the first $n-1$ coordinates of $P_t = (s_t, s_{t+1}, \dots, s_{t+n-1}, 1)$ and maps them to $\sum_{i=0}^{n-2} s_{t+i} p^i \in \mathbb{Z}_{p^{n-1}}$. There are p^{n-1} distinct $z_i \in \mathbb{Z}_{p^{n-1}}$ and for each $z_i \neq 0$, there are p points $Z_i = \{P_{t_0}, \dots, P_{t_{p-1}}\} = \{(s_t, s_{t+1}, \dots, s_{t+n-2}, \alpha, 1) \mid \alpha \in \text{GF}(p)\}$ which are mapped to z_i by σ_{n-1}. For $z_i = 0$ there are $p-1$ corresponding points in Z_0 since the all-zero state does not occur in an m-sequence.

It is not hard to see that the sets $Z_0 \cup \{\infty\}$, $Z_1, \ldots Z_{p^{n-1}-1}$ form the set of parallel (affine) lines through the point $(0, \ldots, 0, 1, 0) \in \mathcal{H}_\infty$, since $Z_i = \{(s_t, \ldots s_{t+n-2}, \alpha, 1) \mid \alpha \in \mathrm{GF}(p)\}$ for some $(n-1)$-tuple $(s_t, \ldots, s_{t+n-2})$ and this forms a line with $(0, \ldots, 0, 1, 0) \in \mathcal{H}_\infty$ (the line defined by the $n-1$ hyperplanes $x_0 - s_t x_n = 0$, $x_1 - s_{t+1} x_n = 0$, ..., $x_{n-2} - s_{t+n-2} x_n = 0$.) This is precisely the construction given by [5] described in Section 3. For each $Z_i = \{P_{t_0}, \ldots, P_{t_{p-1}}\}$, $i = 1, \ldots, p^{n-1} - 1$, let $D_i = \{t_0, \ldots, t_{p-1}\}$, and for $Z_0 = \{P_{t_0}, \ldots, P_{t_{p-2}}\}$, let $D_0 = \{t_0, \ldots, t_{p-2}\}$. Then the sets D_i form a partition type perfect internal $\mathrm{DDF}(p^n; p-1, p, \ldots, p)$ over $\mathbb{Z}_{p^n}$ with $|\mathcal{I}(d)| = p - 1$ for all $d \in \mathbb{Z}_{p^n}^*$.

Similarly, for σ_k, $1 \le k \le n-1$, the set of points $Z_i = \{(s_t, \ldots s_{t+n-k-1}, \alpha_1, \ldots, \alpha_k, 1) \mid \alpha_1, \ldots, \alpha_k \in \mathrm{GF}(p)\}$ correponding to each $z_i \in \mathbb{Z}_{p^k}$ form an $(n-k)$-dimensional subspace and the set of Z_i forms a parallel classes. These are the constructions of [5, Lemma 3.1, 3.2].

Example 4.1. Let $S = (s_t)$ be an m-sequence over GF(3) satifying the linear reccurence relation $x_{t+3} = 2x_t + x_{t+2}$. The state update matrix is therefore

$$C = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

The impulse response sequence is $S = (001110211210100222012212 02)$, and the σ_3-, σ_2- and σ_1-transformations give

P_t	$s(t,3)$	$s(t,3)\sigma_3$	$s(t,2)$	$s(t,2)\sigma_2$	$s(t,1) = s(t,1)\sigma_1$
P_0	001	9	00	0	0
P_1	011	12	01	3	0
P_2	111	13	11	4	1
P_3	110	4	11	4	1
P_4	102	19	10	1	1
P_5	021	15	02	6	0
P_6	211	14	21	5	2
P_7	112	22	11	4	1
P_8	121	16	12	7	1
P_9	210	5	21	5	2
P_{10}	101	10	10	1	1
P_{11}	010	3	01	3	0
P_{12}	100	1	10	1	1
P_{13}	002	18	00	0	0
P_{14}	022	24	02	6	0
P_{15}	222	26	22	8	2
P_{16}	220	8	22	8	2
P_{17}	201	11	20	2	2
P_{18}	012	21	01	3	0
P_{19}	122	25	12	7	1
P_{20}	221	17	22	8	2
P_{21}	212	23	21	5	2
P_{22}	120	7	12	7	1
P_{23}	202	20	20	2	2
P_{24}	020	6	02	6	0
P_{25}	200	2	20	2	2

Writing this in $PG(3,3)$, $P_t = (s_t, s_{t+1}, s_{t+2}, 1)$, and $\mathcal{H}_\infty$ is the hyperplane $x_3 = 0$, and ∞ is the point $(0,0,0,1)$. The projectivity τ maps P_t to P_{t+1}, where τ is represented by the matrix A,

$$A = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The σ_2 transformation maps 3 points to every $z_i \in \mathbb{Z}_9^*$. These form the affine lines of $PG(3,3)$ through the point $(0,0,1,0)$. For example, the points P_1, P_{11}, P_{18} lie on the line defined by $x_0 = 0$, $x_1 - x_3 = 0$. The set $\{1, 11, 18\}$ would be one of the subsets of the difference family. This gives $Q_0 = \{0, 13\}$, $Q_1 = \{1, 11, 18\}$, $Q_2 = \{5, 14, 24\}$, $Q_3 = \{4, 10, 12\}$, $Q_4 = \{2, 3, 7\}$, $Q_5 = \{8, 19, 22\}$, $Q_6 = \{17, 23, 25\}$, $Q_7 = \{6, 9, 21\}$, $Q_8 = \{15, 16, 20\}$.

The σ_1 transformation maps 9 points to every $z_i \in \mathbb{Z}_3^*$. These form the affine planes of $PG(3,3)$ through the point $(0,0,1,0)$. For example, the points $P_2, P_3, P_4, P_7, P_8, P_{10}, P_{12}, P_{19}, P_{22}$ lie on the plane $x_0 - x_3 = 0$. The sets $Q_0 = \{0,1,5,11,13,14,18,24\}$, $Q_1 = \{2,3,4,7,8,10,12,19,22\}$, $Q_2 = \{6,9,15,16,17,20,21,23,25\}$ form a difference family over $\mathbb{Z}_3$.

□

4.3 The other way round?

We see that the m-sequence constructions of [8] gives the projective geometry constructions of [5]. Here we consider how the constructions of [5] relate to m-sequences.

In $PG(n,q)$ we may choose any $n+2$ points (every set of $n+1$ of which are independent) as the simplex of reference (there is an automorphism that maps any set of such $n+2$ points to any other set). Hence we may choose the hyperplane $x_n = 0$ (denoted $\mathcal{H}_\infty$) and the point $(0,0,\ldots,0,1)$ (denoted ∞).

Now, consider a projectivity τ represented by an $(n+1)\times(n+1)$ matrix A that fixes $\mathcal{H}_\infty$ and ∞. It must take the form

$$A = \begin{pmatrix} & & & 0 \\ & C & & \vdots \\ & & & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix},$$

and we see that

$$A^i = \begin{pmatrix} & & & 0 \\ & C^i & & \vdots \\ & & & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix}.$$

So the order of A is given by the order of C. Let the characteristic polynomial of C be $f(x)$. The order of A is hence the order of $f(x)$.

Consider the action of $\langle\tau\rangle$ on the points of $PG(n,q) \setminus (\mathcal{H}_\infty \cup \infty)$. For $\langle\tau\rangle$ to act transitively on these points A must have order $q^n - 1$, which means that $f(x)$ must be primitive. If we use this $f(x)$ as the characteristic polynomial for an LFSR we generate an m-sequence, as in Section 4.1. For prime fields, this is precisely the construction of [8].

Projectivities in the same conjugacy classes have matrices that are similar and therefore have the same characteristic polynomial. There are $\frac{\phi(q^n-1)}{n}$ primitive polynomials of degree n over GF(q) and this gives the number of conjugacy classes of projectivities fixing $\mathcal{H}_\infty$ and ∞ and acting transitively on the points of $PG(n,q) \setminus (\mathcal{H}_\infty \cup \infty)$.

For a particular $\langle\tau\rangle$ with characteristic polynomial $f(x)$ and difference family $\{Q_0, \ldots, Q_{q^{n-1}-1}\}$, there are $q^n - 1$ choices for the point P_0 to be designated 0 in the construction described in Section 3. Each choice gives $Q_i + d$ for each Q_i, $i = 1, \ldots, q^{n-1} - 1$, $d \in \mathbb{Z}_{q^n-1}^*$. This corresponds to the $q^n - 1$ shifts of the m-sequence generated by the LFSR with characteristic polynomial $f(x)$. The choice of parallel class (the point $P_\infty \in \mathcal{H}_\infty$) gives the difference family $\{Q_i + d \ : \ d \in \mathbb{Z}_{q^n-1}, i = 1, \ldots, q^{n-1} - 1\}$. (There are $q-1$ values of d such that $\{Q_i + d\} = \{Q_i\}$.) This corresponds to a permutation of symbol and a shift of the m-sequence. If the set of shifts of an m-sequence is considered as a cyclic code over GF(q) then this gives equivalent codes (more on this in Section 5). The group $\langle\tau\rangle$ has $\phi(q^n - 1)$ generators, and each of the generator τ^i, $(i, q^n - 1) = 1$ corresponds to a multiplier w such that $\{wQ_i \ : \ i = 1, \ldots, q^{n-1} - 1\} = \{Q_i \ : \ i = 1, \ldots, q^{n-1} - 1\}$.

We have described this correspondence in terms of the lines of $PG(n,q)$ but this also applies to the correspondence between higher dimensional subspaces and the σ_k-transformations.

Example 4.2. In $PG(3,3)$, the group of perspectivity generated by τ, represented by the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

fixes the plane $x_3 = 0$ and fixes the point $\infty = (0,0,0,1)$. An affine point $(x,y,z,1)$ is mapped to the point $(y, x+z, y+z, 1)$ and a plane $[a,b,c,d]$ is mapped to the plane $[a+b-c, a, -a+c, d]$. Taking the point $(1,0,0,1)$

as 0, we have the affine lines through $P_\infty = (1,0,0,0)$ in $x_3 = 0$ as

$$\begin{array}{lll} Q_0 = \{0,13\}, & Q_1 = \{1,19,4\}, & Q_2 = \{2,22,23\}, \\ Q_3 = \{3,5,12\}, & Q_4 = \{6,14,17\}, & Q_5 = \{7,11,21\}, \\ Q_6 = \{8,24,20\}, & Q_7 = \{9,10,15\}, & Q_8 = \{16,18,25\}. \end{array}$$

If we consider the action of τ^5, we have

$$\begin{array}{lll} Q'_0 = \{0,13\} = Q_0 \times 7, & Q'_1 = \{6,9,21\} = Q_3 \times 7, & Q'_2 = \{16,20,15\} = Q_4 \times 7, \\ Q'_3 = \{11,1,18\} = Q_7 \times 7, & Q'_4 = \{22,8,19\} = Q_8 \times 7, & Q'_5 = \{17,23,25\} = Q_5 \times 7, \\ Q'_6 = \{12,10,4\} = Q_6 \times 7, & Q'_7 = \{2,3,7\} = Q_1 \times 7, & Q'_8 = \{24,14,5\} = Q_2 \times 7. \end{array}$$

If we choose a different parallel class, say, $P'_\infty = (0,0,1,0)$, we will instead have

$$\begin{array}{lll} Q''_0 = \{10,23\}, & Q''_1 = \{1,24,16\}, & Q''_2 = \{2,0,9\}, \\ Q''_3 = \{3,14,11\}, & Q''_4 = \{4,8,18\}, & Q''_5 = \{5,17,21\}, \\ Q''_6 = \{6,7,12\}, & Q''_7 = \{13,15,22\}, & Q''_8 = \{19,20,25\}, \end{array}$$

and $\{Q'_0, \ldots, Q'_8\} = \{Q_0 + 10, \ldots, Q_8 + 10\}$.

The characteristic polynomial of A is $f(x) = x^3 - x^2 - 2x - 2$. Using $f(x)$ as the characteristic polynomial of an LFSR we have the update matrix C as

$$C = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}.$$

Using the process described in Section 4.2, we obtain (with $(0,0,1,1)$ as 0) the difference family $\{Q_i - 1 \ : \ i = 0, \ldots 8\}$. □

It is clear from this correspondence that the m-sequence constructions of [8] also works over a non-prime field. The σ_k transform is essentially assigning a unique symobl to each k-tuple from the initial m-sequence.

5 Equivalence of FH sequences

In [5], Fuji-Hara *et al.* state "Often we are interested in properties of FH sequences, such as auto-correlation, randomness and generating method, which remain unchanged when passing from one FH sequence to another that is essentially the same. Providing an exact definition for this concept and enumerating how many non 'essentially the same' FH sequences are also interesting problems deserving of attention." Here we discuss the notion of equivalence of FH sequences.

Firstly we adopt the notation of [10] for freqency hopping schemes: An (n, M, q)-frequency hopping scheme (FHS) $\mathcal{F}$ is a set of M words of length n over an alphabet of size q. Each word is an FH sequence.

Elements of the symmetric group S_n can act on $\mathcal{F}$ by permuting the coordinate positions of each word in $\mathcal{F}$. Let ρ_n denote the permutation $\begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix} \in S_n$. We say that an element of S_n is a *rotation* if it belongs to $\langle \rho_n \rangle$, the subgroup generated by ρ_n.

Example 5.1. *Consider the binary $(7,1,2)$-FHS $\mathcal{F}$ consisting of the single word $(0,0,0,1,0,1,1)$. We have $(0,0,0,1,0,1,1)^{\rho_7} = (1,0,0,0,1,0,1)$.*

Definition 5.2. *Let Q be a finite alphabet. Given a set $S \subseteq Q^n$ we define the* rotational closure *of S to be the set*

$$\overset{\Leftrightarrow}{S} = \{\mathbf{w}^\sigma \mid \mathbf{w} \in S, \ \sigma \in \langle \rho_n \rangle\}.$$

If $\overset{\Leftrightarrow}{S} = S$ then we say that S is rotationally closed.

Example 5.3. *Consider the binary $(7,1,2)$-FHS $\mathcal{F}$ consisting of the single word $(0,0,0,1,0,1,1)$. Its rotational closure is the orbit of the word $(0,0,0,1,0,1,1)$ under action by the subgroup $\langle \rho_7 \rangle$:*

$$\begin{aligned} \overset{\Leftrightarrow}{\mathcal{F}} = \{&(0,0,0,1,0,1,1), \\ &(1,0,0,0,1,0,1), \\ &(1,1,0,0,0,1,0), \\ &(0,1,1,0,0,0,1), \\ &(1,0,1,1,0,0,0), \\ &(0,1,0,1,1,0,0), \\ &(0,0,1,0,1,1,0)\}. \end{aligned}$$

If $\mathcal{F}$ is a FHS then $\overset{\Leftrightarrow}{\mathcal{F}}$ is precisely the set of sequences available to users for selecting frequencies. An important property of a FHS is the Hamming correlation properties of the sequences in $\mathcal{F}$.

Let $\mathcal{F}$ be an (n, M, q)-FHS and let $\mathbf{x} = \{x_0, \ldots, x_{n-1}\}$, $\mathbf{y} = \{y_0, \ldots, y_{n-1}\} \in \mathcal{F}$. The Hamming correlation $H_{\mathbf{x},\mathbf{y}}(t)$ at relative time delay t, $0 \leq t < n$, between $\mathbf{x}$ and $\mathbf{y}$ is

$$H_{\mathbf{x},\mathbf{y}}(t) = \sum_{i=0}^{n-1} h(x_i, y_{i+t}),$$

where

$$h(x, y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

Note that the operations on indices are performed modulo n. If $\mathbf{x} = \mathbf{y}$ then $H_{\mathbf{x}}(t) = H_{\mathbf{x},\mathbf{x}}(t)$ is the Hamming auto-correlation. The maximum out-of-phase Hamming auto-correlation of $\mathbf{x}$ is

$$H(\mathbf{x}) = \max_{1 \leq t < n} \{H_{\mathbf{x}}(t)\}$$

and the maximum Hamming cross-correlation between any two distinct FH sequences $\mathbf{x}$, $\mathbf{y}$ is

$$H(\mathbf{x}, \mathbf{y}) = \max_{0 \leq t < v} \{H_{\mathbf{x},\mathbf{y}}(t)\}.$$

We define the maximum Hamming correlation of an (n, M, q)-FHS $\mathcal{F}$ as

$$M(\mathcal{F}) = \max_{\mathbf{x},\mathbf{y} \in \mathcal{F}} \{H(\mathbf{x}), H(\mathbf{y}), H(\mathbf{x}, \mathbf{y})\}.$$

Theorem 5.4. *Let $\mathbf{w} \in Q^n$. The maximum out-of-phase Hamming auto-correlation of $\mathbf{w}$, $H(\mathbf{w})$, is equal to $n - d$, where d is the minimum (Hamming) distance of $\overset{\Leftrightarrow}{\mathbf{w}}$.*

Theorem 5.5. *Let $\mathcal{F}$ be an (n, M, q)-FHS. The minimum distance of $\overset{\Leftrightarrow}{\mathcal{F}}$ is equal to $n - M(\mathcal{F})$.*

The proofs of these theorems are trivial, but the theorems suggest that taking the rotational closure of a frequency hopping sequence allows us to work with the standard notion of Hamming distance in place of the Hamming correlation.

Theorem 5.6. *Let $\mathbf{w} \in Q^n$. If $|\overset{\Leftrightarrow}{\mathbf{w}}| < n$ then $H(\mathbf{w}) = n$.*

Proof. We observe that $|\overset{\Leftrightarrow}{\mathbf{w}}|$ is the size of the orbit of $\mathbf{w}$ under the action of the subgroup $\langle \rho_n \rangle$, which has order n. By the orbit-stabiliser theorem, if $|\overset{\Leftrightarrow}{\mathbf{w}}| < n$ then the stabiliser of $\mathbf{w}$ is nontrivial. That is, there is some (non-identity) rotation that maps $\mathbf{w}$ onto itself. This implies that its maximum out-of-phase Hamming auto-correlation is n. □

In other words, unless a given sequence of length n has worst possible Hamming auto-correlation, its rotational closure always has size n.

The following lemma is also straightforward to prove:

Lemma 5.7. Let $\mathbf{w} \in Q^n$. If $|\overset{\Leftrightarrow}{\mathbf{w}}| < n$ then for $i = 0, 1, \ldots, n-1$ we have $\overset{\Leftrightarrow}{\mathbf{w}^{\rho_n^i}} = \overset{\Leftrightarrow}{\mathbf{w}}$. □

In coding theory, two codes are equivalent if one can be obtained from the other by a combination of applying an arbitrary permutation to the alphabet symbols in a particular coordinate position and/or permuting the coordinate positions of the codewords. These are transformations that preserve the Hamming distance between any two codewords. In the case of frequency hopping sequences, it is the maximum Hamming correlation that we wish to preserve. This is a stronger condition, and hence the set of transformations that are permitted in the definition of equivalence will be smaller. For example, we can no longer apply different permutations to the alphabet in different coordinate positions, as that can alter the out-of-phase Hamming correlations. Because the rotation of coordinate positions is inherent to the definition of Hamming correlation, if we wish to permute the alphabet symbols then we must apply the same permutation to the symbols in each coordinate position. Similarly, not all permutations of columns preserve the out-of-phase Hamming auto-correlation of a sequence.

Example 5.8. *Consider the sequence $(0, 0, 0, 1, 0, 1, 1)$. Its maximum out-of-phase Hamming auto-correlation is 3. However, if we swap the first and last column we obtain the sequence $(1, 0, 0, 1, 0, 1, 0)$, which has maximum out-of-phase Hamming auto-correlation 5.*

However, we can use the notion of rotational closure to determine an appropriate set of column permutations that will preserve Hamming correlation. Recall that for a given word, its out-of-phase Hamming auto-correlation is uniquely determined by the minimum distance of its rotational closure. Now, any permutation of columns preserves Hamming distance, so if we can find a set of permutations that preserve the property of being rotationally closed, then these will in turn preserve the out-of-phase Hamming auto-correlation of individual sequences.

Suppose a word $\mathbf{w}$ of length n has $H(\mathbf{w}) < n$. Then its rotational closure consists of the elements

$$\overset{\Leftrightarrow}{\mathbf{w}} = \{\mathbf{w}, \mathbf{w}^{\rho_n}, \mathbf{w}^{\rho_n^2}, \ldots, \mathbf{w}^{\rho_n^{n-1}}\}.$$

Applying a permutation $\gamma \in S_n$ to the columns of these words gives the set

$$\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} = \{\mathbf{w}^{\gamma}, \mathbf{w}^{\rho_n\gamma}, \mathbf{w}^{\rho_n^2\gamma}, \ldots, \mathbf{w}^{\rho_n^{n-1}\gamma}\}.$$

We wish to establish conditions on γ that ensure that $\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma}$ is itself rotationally closed.

Theorem 5.9. *Suppose $\mathbf{w} \in Q^n$ has out-of-phase Hamming auto-correlation less than n. Then $\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma}$ is rotationally closed if and only if $\gamma \in N_{S_n}(\langle\rho_n\rangle)$, that is γ is an element of the normaliser of $\langle\rho_n\rangle$ in S_n.*

Proof. Suppose $\gamma \in N_{S_n}(\langle\rho_n\rangle)$. Then $\gamma\langle\rho_n\rangle\gamma^{-1} = \langle\rho_n\rangle$. This implies that

$$\overset{\Leftrightarrow}{\mathbf{w}} = \{\mathbf{w}^{\gamma\rho_n^i\gamma^{-1}} \mid i = 0, 1, 2, \ldots, n-1\},$$

and so

$$\begin{aligned}\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} &= \{\mathbf{w}^{\gamma\rho_n^i} \mid i = 0, 1, 2, \ldots, n-1\},\\ &= \overset{\Leftrightarrow}{\mathbf{w}^{\gamma}}.\end{aligned}$$

Conversely, if $\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma}$ is rotationally closed, then

$$\begin{aligned}\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} &= \{\mathbf{w}^{\gamma}, \mathbf{w}^{\rho_n\gamma}, \mathbf{w}^{\rho_n^2\gamma}, \ldots, \mathbf{w}^{\rho_n^{n-1}\gamma}\}\\ &= \{\mathbf{w}', \mathbf{w}'^{\rho_n}, \mathbf{w}'^{\rho_n^2}, \ldots, \mathbf{w}'^{\rho_n^{n-1}}\}\end{aligned}$$

where $\mathbf{w}' = \mathbf{w}^{\rho_n^i\gamma}$ for some i. So we have

$$\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} = \{\mathbf{w}^{\rho_n^i\gamma}, \mathbf{w}^{\rho_n^i\gamma\rho_n}, \mathbf{w}^{\rho_n^i\gamma\rho_n^2}, \ldots, \mathbf{w}^{\rho_n^i\gamma\rho_n^{n-1}}\}.$$

This means that $\mathbf{w}^{\gamma} = \mathbf{w}^{\rho_n^i\gamma\rho_n^j}$ for some j, and so $\mathbf{w}^{\gamma\rho_n^{-j}\gamma^{-1}} = \mathbf{w}^{\rho_n^i}$. Clearly this applies to all i, j, and we have $\gamma \in N_{S_n}(\langle\rho_n\rangle)$. □

Example 5.10. *Consider the permutation $\gamma = (2\quad 5\quad 3)(4\quad 6\quad 7) \in S_7$. We have $\gamma^{-1} = (2\quad 3\quad 5)(4\quad 7\quad 6)$, and*

$$\begin{aligned}\gamma\rho_7\gamma^{-1} &= (2\quad 5\quad 3)(4\quad 6\quad 7)(1\quad 2\quad 3\quad 4\quad 5\quad 6\quad 7)(2\quad 3\quad 5)(4\quad 7\quad 6),\\ &= (1\quad 3\quad 5\quad 7\quad 2\quad 4\quad 6),\\ &= \rho_7^2.\end{aligned}$$

Since ρ_7^2 generates $\langle\rho_7\rangle$ this shows that $\gamma \in N_{S_7}(\langle\rho_7\rangle)$.

Now consider the word (A, B, C, D, E, F, G). The rows of the following matrix give its rotational closure:

$$\begin{bmatrix} A & B & C & D & E & F & G\\ G & A & B & C & D & E & F\\ F & G & A & B & C & D & E\\ E & F & G & A & B & C & D\\ D & E & F & G & A & B & C\\ C & D & E & F & G & A & B\\ B & C & D & E & F & G & A \end{bmatrix}.$$

If we apply γ to the columns of this matrix, we obtain

$$\begin{bmatrix} A & C & E & G & B & D & F \\ G & B & D & F & A & C & E \\ F & A & C & E & G & B & D \\ E & G & B & D & F & A & C \\ D & F & A & C & E & G & B \\ C & E & G & B & D & F & A \\ B & D & F & A & C & E & G \end{bmatrix},$$

which is easily seen to be the rotational closure of any of its rows.

We now look at applying these ideas to the sequence $(0,0,0,1,0,1,1)$. Permuting its columns with γ in fact yields $(0,0,0,1,0,1,1)$, which is trivially equivalent to the original sequence. Less trivially, $\begin{pmatrix} 2 & 4 & 3 & 7 & 5 & 6 \end{pmatrix}$ is another example of an element of the normaliser of $\langle\rho_7\rangle$, and applying this permutation to the columns yields the sequence $(0,1,1,0,1,0,0)$. This is an example of an 'equivalent' frequency hopping sequence that is not simply a rotation of the original sequence.

Definition 5.11. *We say that two (n,M,q)-FHSs are* equivalent *if one can be obtained from the other by a combination of permuting the symbols of the underlying alphabet and/or applying to the columns of its sequences any permutation that is an element of $N_{S_n}(\langle\rho_n\rangle)$.*

Equivalent FHSs have the same maximum Hamming correlation.

5.1 Comparison with the notion of equivalence for DDFs

Two distinct difference families are said to be equivalent if there is an isomorphism between the underlying groups that maps one DDF onto a translation of the other. In Section 2.1 we discussed the correspondence between a partition type DDF and an FHS. In fact, we will see that two partition type DDFs over $\mathbb{Z}_n$ are equivalent in this sense if and only if the corresponding FHSs are equivalent in the sense of Definition 5.11. We begin by noting that the automorphism group of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^*$. As in Section 5 let $\rho_n \in S_n$ be the permutation $\begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix}$. Any element $\gamma \in N_{S_n}(\langle\rho_n\rangle)$ induces a map $\phi_\gamma \colon \mathbb{Z}_n \to \mathbb{Z}_n$ by sending $i \in \mathbb{Z}_n$ to the unique element $j \in \mathbb{Z}_n$ for which $\gamma^{-1}\rho_n^i\gamma = \rho^j$. The map ϕ_γ is a homomorphism, since if $\phi_\gamma(i_1) = j_1$ and $\phi_\gamma(i_2) = j_2$ then $\gamma^{-1}\rho_n^{i_1+i_2}\gamma = \gamma^{-1}\rho_n^{i_1}\gamma\gamma^{-1}\rho_n^{i_2}\gamma = \rho_n^{j_1}\rho_n^{j_2} = \rho_n^{j_1+j_2}$, so $\phi_\gamma(i_1+i_2) = \phi_\gamma(i_1) + \phi_\gamma(i_2)$; in fact it is an automorphism. Every automorphism of $\langle\rho_n\rangle$ can be obtained in this fashion.

Theorem 5.12. *Let $\mathcal{F}$ be a length n FHS consisting of a single word, and let $\mathcal{D}$ be the corresponding partition type* DDF *over $\mathbb{Z}_n$. Then the FHS obtained by applying a permutation $\gamma \in N_{S_n}(\langle\rho\rangle)$ to the coordinate positions of $\mathcal{F}$ corresponds to a* DDF *that is a translation of the* DDF *obtained from $\mathcal{D}$ by applying the automorphism ϕ_γ to the elements of $\mathbb{Z}_n$.*

Proof. It is a straightforward calculation to verify that $\gamma^{-1}\rho_n\gamma$ is the cycle $\begin{pmatrix} 1^\gamma & 2^\gamma & \ldots & n^\gamma \end{pmatrix}$. For $\gamma \in N_{S_n}(\langle\rho_n\rangle)$ this is equal to ρ_n^k for some k. It follows that for $i = 1, 2, \ldots, n-1$ we have

$$(i+1)^\gamma = i^\gamma + k. \tag{3}$$

The correspondence between $\mathcal{F}$ and $\mathcal{D}$ is obtained by associating positions in the sequence with elements of $\mathbb{Z}_n$. For example, the FHS $\mathcal{F} = (1,1,2,3,2)$ corresponds to the DDF $(\mathbb{Z}_5; \{0,1\}, \{2,4\}, \{3\})$:

$\mathbb{Z}_5$	0	1	2	3	4
$\mathcal{F}$	1	1	2	3	2

We observe that in this representation, the $i+1^{\text{th}}$ element of the sequence $\mathcal{F}$ is in correspondence with the element $i-1 \in \mathbb{Z}_n$. If we apply γ to the positions of $\mathcal{F}$, then the entry in the $j+1^{\text{th}}$ position is mapped to the $i+1^{\text{th}}$ position when $(j+1)^\gamma = i+1$. Repeatedly applying the relation in (3) tells us that in this case we have $i+1 = 1^\gamma + jk$, so $i = (1^\gamma - 1) + jk$.

If we apply ϕ_γ to $\mathbb{Z}_n$ then element $j \in \mathbb{Z}_n$ is replaced by element i when $\gamma^{-1}\rho_n^j\gamma = \rho^i$. But we have that

$$\begin{aligned} \gamma^{-1}\rho_n^j\gamma &= (\gamma^{-1}\rho\gamma)^j, \\ &= (\rho_n^k)^j, \\ &= \rho_n^{kj}, \end{aligned}$$

so it must be the case that $i = kj$. It follows that if we then translate this DDF by adding $1^\gamma - 1$ to each element of $\mathbb{Z}$ we obtain the same overall transformation that was effected by applying γ to $\mathcal{F}$. □

Example 5.13. For example, let $\gamma = \begin{pmatrix} 1 & 5 & 3 & 4 \end{pmatrix} \in N_{S_5}(\langle \rho_5 \rangle)$. Applying γ to $\mathcal{F} = (1, 1, 2, 3, 2)$ we have

$$\begin{array}{c|ccccc} \mathbb{Z}_5 & 0 & 1 & 2 & 3 & 4 \\ \hline \mathcal{F}^\gamma & 3 & 1 & 2 & 2 & 1 \end{array},$$

with resulting FHS $(3, 1, 2, 2, 1)$ and corresponding DDF $(\mathbb{Z}_5; \{0\}, \{1, 4\}, \{2, 3\})$. We observe that $1^\gamma = 5$, so that $1^\gamma - 1 = 4$. Alternatively, we note that $\gamma^{-1}\rho_5\gamma = \begin{pmatrix} 1 & 3 & 5 & 2 & 4 \end{pmatrix} = \rho_5^2$. Hence ϕ_γ gives

$$\begin{array}{c|ccccc} \phi_\gamma(\mathbb{Z}_5) & 0 & 2 & 4 & 1 & 3 \\ \hline \mathcal{F} & 1 & 1 & 2 & 3 & 2 \end{array},$$

which we can rewrite in order as

$$\begin{array}{c|ccccc} \phi_\gamma(\mathbb{Z}_5) & 0 & 1 & 2 & 3 & 4 \\ \hline \mathcal{F} & 1 & 3 & 1 & 2 & 2 \end{array}.$$

The resulting FHS is $(1, 3, 1, 2, 2)$, which is simply a cyclic shift of the one obtained previously. The DDF is $(\mathbb{Z}_5; \{1\}, \{0, 2\}, \{3, 4\})$. If we add 4 to each element, we recover the previous DDF. □

6 Conclusion

We have given a general definition of a disjoint difference family, and have seen a range of examples of applications in communications and information security for these difference families, with different applications placing different constraints on the associated properties and parameters. Focussing on the case of FHSs and their connection with partition-type disjoint difference families, we have shown that a construction due to Fuji-Hara *et al.* [5] gives rise to precisely the same disjoint difference families as an eariler construction of Lempel and Greenberger [8], thus answering an open question in [5]. In response to the question of Fuji-Hara *et al.* as to when two FHSs can be considered to be "essentially the same" we have established a notion of equivalence of frequency hopping schemes. FHSs based on a single sequence corrrespond to partition-type disjoint difference families, and in this case we have shown that our definition of equivalence corresponds to an established notion of equivalence for difference families, although our definition also applies more generally to schemes based on more than one sequence. An interesting avenue for further research would be to determine whether a more general notion of difference family could be used to give insight into the construction and analysis of FHSs based on more than one sequence.

References

[1] F. R. K. Chung, J. A. Salehi, and V. K. Wei. Optical orthogonal codes: design, analysis and applications. *IEEE Transactions on Information Theory*, 35(3):595–604, May 1989.

[2] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC, 2nd edition, 2006.

[3] R. Cramer, S. Fehr, and C. Padró. Algebraic manipulation detection codes. *Science China Mathematics*, 56(7):1349–1358, 2013.

[4] R. C. Dixon. *Spread Spectrum Systems*. Wiley-Blackwell, 2nd edition, 1984.

[5] R. Fuji-Hara, Y. Miao, and M. Mishima. Optimal frequency hopping sequences: a combinatorial approach. *IEEE Transactions on Information Theory*, 50(10):2408–2420, Oct 2004.

[6] Y. Fujiwara and V. D. Tonchev. High-rate self-synchronizing codes. *IEEE Transactions on Information Theory*, 59(4):2328–2335, April 2013.

[7] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs, 2nd edition, 1998.

[8] A. Lempel and H. H. Greenberger. Families of sequences with optimal hamming-correlation properties. *Information Theory, IEEE Transactions on*, 20(1):90–94, Jan 1974.

[9] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its applications*. Cambridge University Press, Cambridge, UK, 2nd edition, 1997.

[10] M. Nyirenda, S. L. Ng, and K. M. Martin. A combinatorial model of interference in frequency hopping schemes. *CoRR*, 2015. Submitted to Designs, Codes and Cryptography.

[11] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Mathematics*, 279(13):383–405, 2004. In Honour of Zhu Lie.

[12] M. B. Paterson and D. R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *CoRR*, abs/1506.02711, 2015.

[13] V. D. Tonchev. Difference systems of sets and code synchronization. *Rendiconti del Seminario Matematico di Messina Series II*, 9:217226, 2003.